(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 098 472 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
09.05.2001 Patentblatt 2001/19

(51) Int. Cl.[7]: **H04L 9/32**

(21) Anmeldenummer: **00123821.1**

(22) Anmeldetag: **02.11.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **03.11.1999 DE 19952841**

(71) Anmelder: **TeraTron GmbH**
51647 Gummersbach (DE)

(72) Erfinder:
- **Weiss, Bernd**
  51647 Gummersbach (DE)
- **Konrad, Reimund**
  51647 Gummersbach (DE)
- **Petsching, Wilfried**
  51702 Bergneustadt (DE)

(74) Vertreter: **Cohausz & Florack**
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(54) Chip für die Speicherung eines Secret Keys zur Verwendung in einer Nutzungsberechtigungskontrolleinrichtung

(57) Die Erfindung betrifft einen Chip für die Speicherung eines Secret Keys zur Verwendung durch einen Verschlüsselungsalgorithmus 24 zum Erzeugen einer verschlüsselten Nachricht in einer Nutzungsberechtigungskontrolleinrichtung. Um die durch eine Nutzungsberechtigungskontrolleinrichtung gewährte Sicherheit zu erhöhen, umfaßt der Chip erfindungsgemäß einen nichtflüchtigen Speicher 20, der mindestens einen Teilbereich 21, 22 aufweist, in dem ein Secret Key gespeichert ist, sowie einen mindestens einen Verschlüsselungsalgorithmus 24 realisierenden Hardwarebereich mit Zugriff zu dem Teilbereich 21, 22 des nichtflüchtigen Speichers 20 mit einem Secret Key.

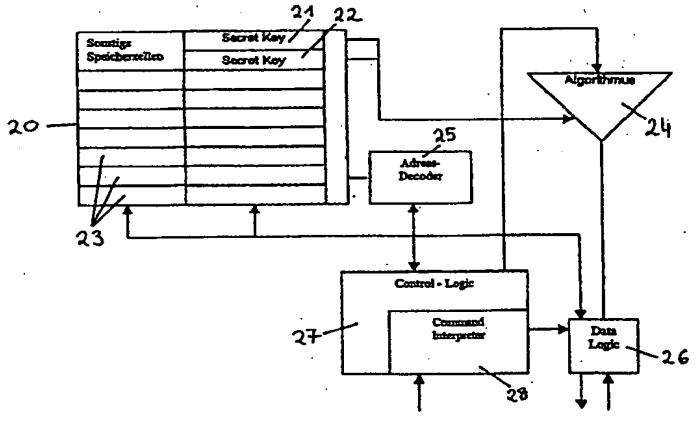

FIG. 3

EP 1 098 472 A2

Beschreibung

[0001] Die Erfindung betrifft einen Chip für die Speicherung eines Secret Keys, der zur Verwendung durch einen Verschlüsselungsalgorithmus zum Erzeugen einer verschlüsselten Nachricht in einer Nutzungsberechtigungskontrolleinrichtung vorgesehen ist.

[0002] Die Kontrolle einer Nutzungsberechtigung von Funktionen einer Einrichtung durch Benutzer oder Gegenstände erfolgt heutzutage häufig über eine automatische Authentifizierung, zu der zwischen einer benutzerseitigen Schlüsseleinrichtung und einer einrichtungsseitigen Auswerte- und Freigabeeinrichtung verschlüsselten Nachrichten, die auf einem „Secret Key" basieren, übertragen werden. Ein Secret Key ist dabei ein geheimer Wert, der sowohl in der Schlüssel- als auch in der Auswerte- und Freigabeeinrichtung gespeichert ist und der selber nie übertragen wird. Die Schlüsseleinrichtung und die Auswerte- und Freigabeeinrichtung stellen zusammen die eingangs genannte Nutzungsberechtigungskontrolleinrichtung dar.

[0003] In einem Kraftfahrzeug kann beispielsweise eine Wegfahrsperre zur Kontrolle der Antriebsfunktionen eine solche Nutzungsberechtigungskontrolleinrichtung darstellen. Die Auswerte- und Freigabeeinrichtung ist dann in dem Fahrzeug integriert, während die Schlüsseleinrichtung von dem Benutzer mitgeführt wird.

[0004] Die Elemente einer entsprechenden Wegfahrsperre sind zur Veranschaulichung schematisch in Figur 1 dargestellt.

[0005] Die fahrzeugseitige Auswerte- und Freigabeeinrichtung 1 weist eine (nicht dargestellte) Antenne und eine damit verbundene Auswerteeinheit 2, einen Bus 3 und eine Antriebssteuereinheit 4, z.B. eine Motormanagementeinheit, auf. Die Auswerteeinheit 2 kann ein eigenständiges Steuergerät darstellen oder in eine andere funktionale Gruppe, wie Anzeigeinstrumente oder Bordcomputer, integriert sein. Über den Bus 3 hat sie Zugang zu der Antriebssteuereinheit 4. Die Schlüsseleinrichtung 5 weist einen Crypt-Transponder auf, der die für Verschlüsselungen notwendige Energie induktiv über die Auswerteeinheit 2 erhält. In der Schlüsseleinrichtung 5, der Auswerteeinheit 2 und der Antriebssteuereinheit 4 ist jeweils ein Secret Key und ein Verschlüsselungsalgorithmus gespeichert.

[0006] Wird von einem Benutzer die Freigabe des Antriebs gewünscht, so authentifiziert zunächst die Auswerteeinheit 2 die von dem Benutzer mitgeführte Schlüsseleinheit 5 mittels einer von der Schlüsseleinheit 5 erhaltenen verschlüsselten Nachricht. Anschließend schaltet die Auswerteeinheit 2 über den Bus 3 die Antriebssteuereinheit 4 mittels einer weiteren verschlüsselten Nachricht frei. Über diese weitere verschlüsselte Nachricht erfolgt gleichzeitig mit der Freigabe der Funktionen auch eine Authentifizierung der Auswerteeinheit 2 gegenüber der Antriebssteuereinheit 4, d.h. auch die Auswerteeinheit 2 muß ihre Berechtigung für die Freischaltung nachweisen. Die Verschlüsselung der Nachrichten wird basierend auf den in den jeweiligen Einrichtungen 2, 4, 5 gespeicherten Secret Keys durch den ebenfalls jeweils vorhandenen Verschlüsselungsalgorithmus erzeugt. Die Authentifizierung kann sowohl zwischen Schlüsseleinrichtung 5 und Auswerteeinheit 2 als auch zwischen Auswerteeinheit 2 und Antriebssteuereinheit 4 einseitig oder zweiseitig erfolgen.

[0007] Der Verschlüsselungsalgorithmus ist üblicherweise als Software ausgebildet und in einem Microcontroller der Auswerteeinheit 2 bzw. der Antriebssteuereinheit 4 enthalten. Häufig wird außerdem der im Mikrocontroller enthaltene, nichtflüchtige Speicher zur Speicherung des Secret Keys benutzt. In komplexen Systemarchitekturen weist der Mikrocontroller jedoch oft keinen nichtflüchtigen Speicher auf. In diesem Fall wird der Secret Key in einem externen, nichtflüchtigen Speicher abgelegt. Das bedeutet aber, daß zum einen der nichtflüchtige Speicher leichter ausgetauscht werden kann und daß zum anderen der Secret Key aus dem externen nichtflüchtigen Speicher ausgelesen werden können muß, um ihn der Software mit dem Verschlüsselungsalgorithmus in dem Mikrocontroller zur Verfügung zu stellen. Es sind Fälle bekannt, bei denen die Informationen solcher nichtflüchtigen Speicher ausgelesen und in eine neue Auswerte- oder Antriebssteuereinheit 2, 4 eingespeichert wurden, um den Diebstahl eines Fahrzeuges vorzubereiten und durchzuführen.

[0008] Der Erfindung liegt die Aufgabe zugrunde, die durch eine Nutzungsberechtigungskontrolleinrichtung gewährte Sicherheit weiter zu erhöhen.

[0009] Diese Aufgabe wird erfindungsgemäß gelöst durch einen Chip für die Speicherung eines Secret Keys zur Verwendung durch einen Verschlüsselungsalgorithmus zum Erzeugen einer verschlüsselten Nachricht in einer Nutzungsberechtigungskontrolleinrichtung, umfassend einen nichtflüchtigen Speicher, der mindestens einen Teilbereich aufweist, in dem ein Secret Key gespeichert ist, sowie einen mindestens einen Verschlüsselungsalgorithmus realisierenden Hardwarebereich mit Zugriff zu dem mindestens einen Teilbereich des nichtflüchtigen Speichers mit einem Secret Key.

[0010] Erfindungsgemäß ist der Verschlüsselungsalgorithmus also als Hardware implementiert und außerdem auf dem gleichen Chip integriert wie ein nicht flüchtiger Speicher, der den Secret Key beinhaltet. Im Gegensatz zum Stand der Technik wird der Secret Key somit nicht über einen Ausgang nach außen zugänglich gemacht, um ihn dem Verschlüsselungsalgorithmus zur Verfügung zu stellen. Dadurch wird der Zugang zu dem Secret Key effektiver vor unbefugten Zugriffen geschützt.

[0011] Hinzu kommt, daß die Hardwareverdrahtung auf einem Chip üblicherweise durch Passivierung geschützt sind. Da der Verlauf der Verdrahtung von außen auch nicht unmittelbar ersichtlich ist, ist ein Aus-

lesen des Secret Keys besonders erschwert.

[0012] Die verwendeten Begriffe verschlüsselt und Verschlüsselungsalgorithmus sind weit zu verstehen und beziehen sich auf jegliche Umwandlung einer Nachricht, die auf einem Algorithmus und einem Secret Key basiert. So fällt hierunter erfindungsgemäß auch entschlüsselt bzw. ein Entschlüsselungsalgorithmus. Eine kopiersichere Entschlüsselung kann z.B. von Relevanz sein, wenn für eine Nutzungsberechtigungskontrolle eine verschlüsselt übertragene Nachricht unverschlüsselt mit einer vorhandenen Nachricht verglichen werden soll.

[0013] Bevorzugte Ausgestaltungen des erfindungsgemäßen Chips gehen aus den Unteransprüchen hervor.

[0014] Vorzugsweise ist der Bereich des nichtflüchtigen Speichers, in dem der Secret Key abgelegt ist, nicht auslesbar. Ein Zugriff auf einen nicht lesbarer Bereich eines nichtflüchtigen Speichers kann nur mit erheblichem Aufwand erlangt werden. Die Sicherheit vor einem unbefugten Zugriff auf den Secret Key von außen wird somit auf diese Weise noch weiter erhöht.

[0015] In einer weiter bevorzugten Ausgestaltung des erfindungsgemäßen Chips ist der nichtflüchtige Speicher ein EEPROM, ein Flash-RAM oder ein FRAM.

[0016] Der Inhalt des Bereichs des nichtflüchtigen Speichers mit gespeichertem Secret Key kann entweder änderbar oder nicht änderbar sein. Wenn er nicht änderbar ist, so wird er lediglich einmal während der Produktion programmiert. Wenn er änderbar ist, so kann ein Paßwort vorgesehen sein, mit dem der Secret Key gegen ein unbefugtes Überschreiben geschützt wird.

[0017] Weitere Teilbereich des nichtflüchtigen Speichers können zum Ablegen weiterer Daten verwendet werden, insbesondere für weitere Daten, die ebenfalls von dem Verschlüsselungsalgorithmus eingesetzt werden. Ein Beispiel für solche Daten ist ein Zählerzustand, der verschlüsselt wird. Dabei kann beispielsweise auch ein Inkrementieren oder Dekrementieren des Zählerzustands nur um jeweils eins möglich zugelassen sein.

[0018] Der erfindungsgemäße Chip kann in allen Einrichtungen eingesetzt werden, die ein Verschlüsseln mit einer Verschlüsselungsfunktion basierend auf einem Secret Key vorsehen und bei denen ein unberechtigter Zugang zu dem Secret Key befürchtet werden muß.

[0019] Der Chip kann dabei beispielsweise in einer Auswerteeinheit einer Nutzungsberechtigungskontrolleinrichtung eingesetzt werden, die vorgesehen ist zum Vergleichen einer intern erzeugten verschlüsselten Nachricht mit einer erhaltenen verschlüsselten Nachricht und zum Erzeugen und Abgeben einer weiteren verschlüsselten Nachricht an eine Funktionssteuereinrichtung. Die Funktionssteuereinrichtung steuert dabei die zu schützenden Funktionen, beispielsweise die Antriebsfunktionen eines Kraftfahrzeugs.

[0020] Ebenso kann ein erfindungsgemäßer Chip aber auch alternativ oder zusätzlich in einer Funktionssteuereinrichtung einer Nutzungsberechtigungskontrolleinrichtung zum Vergleichen einer intern erzeugten verschlüsselten Nachricht mit einer erhaltenen verschlüsselten Nachricht und zum Freigeben mindestens einer durch die Nutzungsberechtigungskontrolleinrichtung geschützten Funktion bei übereinstimmenden Nachrichten eingesetzt werden.

[0021] Ein bevorzugtes Einsatzgebiet für den erfindungsgemäßen Chip sind die Elemente der Wegfahrsperre eines Kraftfahrzeugs.

[0022] Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels unter Bezugnahme auf Zeichnungen näher erläutert. Dabei zeigt:

- Fig. 1: schematisch die Elemente einer Wegfahrsperre eines Kraftfahrzeugs,
- Fig. 2: schematisch die Funktionsweise eines erfindungsgemäßen Chips und
- Fig. 3: schematisch den Aufbau eines Chips gemäß Erfindung.

[0023] Figur 1 wurde bereits in der Einleitung beschrieben. Die dargestellte Wegfahrsperre eines Kraftfahrzeugs liegt auch den weiteren Ausführungen zugrunde.

[0024] Figur 2 illustriert die verschiedenen, für die Wegfahrsperre aus Figur 1 durchgeführten Verschlüsselungen, wobei die eingesetzten Verschlüsselungsalgorithmen durch Dreiecke 10-13 symbolisiert sind.

[0025] Auf der linken Seite von Figur 2 ist die Verschlüsselung in der Schlüsseleinrichtung 5 und in der Mitte und auf der rechten Seite die Verschlüsselung in dem Kraftfahrzeug dargestellt. Fahrzeugseitig ist dabei weiter unterschieden zwischen zwei verschiedenen Verschlüsselungen in der Auswerteeinheit 2 und einer Verschlüsselung in der Antriebssteuereinheit 4. Für jede Verschlüsselung wird ein eigener Verschlüsselungsalgorithmus 10-13 eingesetzt, wobei aber die beiden Verschlüsselungen in der Auswerteeinheit 2 auch mit dem gleichen Verschlüsselungsalgorithmus durchgeführt werden können. Die Verschlüsselung wird außerdem nur für eine einseitige Authentifizierung der Schlüsseleinrichtung 5 gegenüber der Auswerteeinheit 2 und der Auswerteeinheit 2 gegenüber der Antriebssteuereinheit 4 beschrieben. Genauso ist aber auch eine jeweils gegenseitige Authentifizierung möglich.

[0026] Jeder der Verschlüsselungsalgorithmen 10-13 erhält als Eingang einen Secret Key 14-17 und einen weiteren Wert X, Y, der verschlüsselt werden soll. Erfindungsgemäß sind dabei die Verschlüsselungsalgorithmen 10-13 hardwaremäßig ausgebildet und auf dem gleichen Chip wie ein nichtflüchtiger Speicher mit dem jeweilig zugeführten, nicht lesbaren Secret Key 14-17 integriert. Als Ausgang liefern die Verschlüsselungsalgorithmen 10-13 eine verschlüsselte Nachricht F(X), H(Y), die eine Funktion von dem jeweiligen eingegebenen Wert X, Y sind und außerdem auf dem jeweiligen

Secret Key 14-17 basieren.

[0027] Der Verschlüsselungsalgorithmus 10 in der Schlüsseleinheit 5 erhält nun zunächst als eingegebenen Wert X eine Zufallsvariable von der Auswerteeinheit 2. Alternativ können auch andere Werte X eingegeben werden, wie ein Zählerstand eines integrierten Zählers, der in Schlüsseleinrichtung 5 und Auswerteeinrichtung 2 gleich variiert wird, so daß keine Übermittlung von der Auswerteeinheit 2 zu der Schlüsseleinrichtung 5 vorausgehen muß. Die Zufallsvariable X wird von dem Verschlüsselungsalgorithmus 10 basierend auf dem in der Schlüsseleinrichtung 5 gespeicherten Secret Key 14 verschlüsselt und an die Auswerteeinheit 2 zurückgesandt.

[0028] Die Auswerteeinheit 2 liefert die gleiche Zufallsvariable X, die sie an die Schlüsseleinrichtung 5 gesandt hatte, auch an ihren ersten eigenen Verschlüsselungsalgorithmus 11. Dieser verschlüsselt die Zufallszahl X seinerseits unter Berücksichtigung des ersten in der Auswerteeinheit 2 gespeicherten Secret Keys 15.

[0029] Stimmt der von der Schlüsseleinrichtung 5 zurück erhaltene, verschlüsselte Wert F(X) mit dem in der Auswerteeinrichtung 2 generierten, verschlüsselten Wert F(X) überein, so verschlüsselt die Auswerteeinheit 2 eine andere, von der Antriebssteuereinheit 4 erhaltenen Zufallszahl Y mittels des zweiten Verschlüsselungsalgorithmus 12 und basierend auf dem zweiten gespeicherten Secret Key 16. Diese zweite verschlüsselte Zufallszahl H(Y) sendet die Auswerteeinheit 2 dann an die Antriebssteuereinheit 4.

[0030] Auch in der Antriebssteuereinheit 4 wird die an die Auswerteeinheit 2 gesendete Zufallszahl Y basierend auf dem dort gespeicherten Secret Key 17 mittels des eigenen Verschlüsselungsalgorithmus 13 verschlüsselt. Stimmen nun der in der Antriebssteuereinheit 4 verschlüsselte Wert H(Y) und der von der Auswerteeinheit 2 erhaltene, verschlüsselte Wert H(Y) überein, so werden die Antriebsfunktionen freigegeben. Der Benutzer kann das Fahrzeug also nun in Betrieb nehmen.

[0031] Die hier beschriebene Freigabe einer Nutzung erfolgte lediglich beispielhaft zur Veranschaulichung. Sie kann auch auf jede beliebige andere Weise erfolgen, solange sie auf verschlüsselten Nachrichten beruht, die mittels eines Secret Keys gebildet werden.

[0032] Figur 3 stellt den Aufbau eines erfindungsgemäßen Chips dar, der in der Auswerteeinheit 2 aus Figur 1 mit einem Verschlüsselungsverfahren ähnlich dem zu Figur 2 beschriebenen eingesetzt wird.

[0033] Ein als EEPROM ausgebildeter, nichtflüchtiger Speicher 20 umfaßt mehrere Speicherzellen 21, 22, 23. Zwei der Speicherzellen 21, 22 sind nicht lesbar und jeweils mit einem Secret Key belegt. Die weiteren Speicherzellen 23 sind lesbar und mit weiteren Daten beschrieben.

[0034] Ein Hardwarebereich, der einen Verschlüsselungsalgorithmus 24 bildet, hat unmittelbaren Zugriff auf den nicht lesbaren Teilbereich 21, 22 des nichtflüchtigen Speichers 20. Als weitere Hardwarebereiche hat ferner ein Adressen-Decodierer 25 Lesezugriff und eine Datenlogik 26 Lese- und Schreibzugang zu den lesbaren Speicherzellen 23. Der Adressen-Decodierer 25 ist außerdem mit einer Steuerlogik 27 verbunden. Auch die Steuerlogik 27 wird durch einen Hardwarebereich des erfindungsgemäßen Chips gebildet. Die Steuerlogik 27 weist einen Bereich zur Befehlsinterpretation 28 auf, in den von außen Befehle eingegeben werden können. Ausgänge der Steuerlogik 27 sind dem Verschlüsselungsalgorithmus 24 und der Datenlogik 26 zugeführt. Die Datenlogik 26 weist eine Schnittstelle nach außen auf, über die Daten ein- und ausgegeben werden können.

[0035] Die Funktionsweise des dargestellten Chips ist die folgende:

[0036] Über den Bereich zur Befehlsinterpretation 28 der Steuerlogik 27 wird ein Befehl zum Generieren einer verschlüsselten Nachricht eingegeben. Der Befehl beinhaltet dabei auch, ob es sich um eine Nachricht für die Authentifizierung der Schlüsseleinrichtung 5 und/oder für eine Authentifizierung der Auswerteeinheit gegenüber der Antriebssteuereinrichtung 4 handeln soll. Die Steuerlogik 27 liest daraufhin über den Adressen-Decodierer 25 für die Verschlüsselung relevante Daten aus den entsprechenden, auslesbaren Zellen 23 des nichtflüchtigen Speichers 20 aus und leitet diese zusammen mit einem Verschlüsselungsbefehl an den Verschlüsselungsalgorithmus 24 weiter. Die für die Verschlüsselung relevante Daten können beispielsweise aus einem Zählerzustand bestehen, der über die Datenlogik 26 in entsprechenden Speicherzellen 23 vor oder nach jeder Verschlüsselung neu gesetzt, insbesondere inkrementiert oder dekrementiert, werden kann. Ebenso können über die Datenlogik 26 Zufallszahlen, die an die Schlüsseleinheit 5 gesandt oder von der Antriebssteuereinheit 4 erhalten wurden, in lesbare Bereiche 23 des nichtflüchtigen Speichers 20 geschrieben und über Adressen-Decodierer 25 und Steuerlogik 27 an den Verschlüsselungsalgorithmus 24 weitergegeben werden.

[0037] Entsprechend dem von der Steuerlogik 27 erhaltenen Befehl erzeugt der Verschlüsselungsalgorithmus 24 auf Grundlage der Secret Keys 15, 16 und der weiteren zugeführten Daten X, Y eine verschlüsselte Nachricht F(X), H(Y) für die Schlüsseleinrichtung 5 und/oder für die Antriebssteuereinrichtung 4. Da hier im Gegensatz zu Figur 2 nur ein Verschlüsselungsalgorithmus 24 für beide Verschlüsselungen eingesetzt wird, sind dabei die der Verschlüsselung zugrunde liegende Funktionen F und H identisch. Über die Datenlogik 26 werden die verschlüsselten Nachrichten F(X), H(Y) ausgegeben. Eine Nachricht für die Schlüsseleinrichtung 5 kann dann beispielsweise in einem Mikrocontroller der Auswerteeinheit 2 mit einer von der Schlüsseleinrichtung 5 empfangenen, verschlüsselten Nachricht F(X) verglichen werden und im Falle einer Übereinstimmung kann eine Nachricht H(Y) zur Authentifizierung gegen-

über der Antriebssteuereinrichtung 4 an diese zur Freischaltung der Antriebsfunktionen übermittelt werden.

[0038] Über die Datenlogik 26 sind auch weitere Daten in den lesbaren Bereich 23 des nichtflüchtigen Speichers 20 schreibbar oder aus diesem lesbar. Das Schreiben kann dabei mit üblichen Adressierungsmethoden erfolgen. Auch eine Neuschreiben der Secret Keys 15, 16 ist möglich, nachdem ein Paßwort eingegeben wurde. Die Befehle zu einer Änderung der Speicherinhalte erhält die Datenlogik 26 über den Bereich zur Befehlsinterpretation 28 der Steuerlogik 27, dem entsprechende Befehle von außen vorgegeben werden. Die erforderlichen Daten werden der Datenlogik 26 direkt von außen zugeführt.

[0039] Insgesamt ist sichergestellt, daß der erfindungsgemäße Chip nur zusammen mit den zum Fahrzeug gehörenden Schlüsseleinrichtungen genutzt werden kann. Denn ein ausgetauschter Chip müßte zur Freigabe der Antriebsfunktionen nicht nur den Verschlüsselungsalgorithmus, sondern zumindest auch den Secret Key für die verschlüsselten Nachrichten zu der Antriebssteuereinheit aufweisen. Ein Zugriff auf die Secret Keys ist aber mit dem erfindungsgemäßen Chip erheblich erschwert.

Patentansprüche

1. Chip für die Speicherung eines Secret Keys (15, 16) zur Verwendung durch einen Verschlüsselungsalgorithmus (11, 12, 24) zum Erzeugen einer verschlüsselten Nachricht in einer Nutzungsberechtigungskontrolleinrichtung, umfassend einen nichtflüchtigen Speicher (20), der mindestens einen Teilbereich (21, 22) aufweist, in dem ein Secret Key (15, 16) gespeichert ist, sowie einen mindestens einen Verschlüsselungsalgorithmus (24) realisierenden Hardwarebereich mit Zugriff zu dem mindestens einen Teilbereich (21, 22) des nichtflüchtigen Speichers (20) mit einem Secret Key (15, 16).

2. Chip nach Anspruch 1,
dadurch gekennzeichnet,
daß der mindestens eine Teilbereich (21, 22) des nichtflüchtigen Speichers (20), in dem ein Secret Key (15, 16) gespeichert ist, nicht lesbar ist.

3. Chip nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
daß der nichtflüchtige Speicher (20) ein EEPROM, ein Flash-RAM oder ein FRAM ist.

4. Chip nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß der Inhalt des mindestens eine Teilbereich (21, 22) des nichtflüchtigen Speichers (20), in dem ein Secret Key (15, 16) gespeichert ist, nicht änderbar ist.

5. Chip nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß der Inhalt des mindestens eine Teilbereich (21, 22) des nichtflüchtigen Speichers (20), in dem ein Secret Key (15, 16) gespeichert ist, erneut beschreibbar ist.

6. Chip nach Anspruch 5,
dadurch gekennzeichnet,
daß der Inhalt des mindestens eine Teilbereich (21, 22) des nichtflüchtigen Speichers (20), in dem ein Secret Key (15, 16) gespeichert ist, mit einem Paßwort gegen ein erneutes Überschreiben geschützt ist.

7. Chip nach einem der voranstehenden Ansprüche,
dadurch gekennzeichnet,
daß in einem weiterer Teilbereich (23) des nichtflüchtigen Speichers (20) weiterer für die Verschlüsselung eingesetzte Daten gespeichert werden.

8. Auswerteeinheit (2) einer Nutzungsberechtigungskontrolleinrichtung zum Vergleichen einer intern erzeugten verschlüsselten Nachricht (F(X)) mit einer erhaltenen verschlüsselten Nachricht (F(X)) und zum Erzeugen und Abgeben einer weiteren verschlüsselten Nachricht (H(Y)) an eine Funktionssteuereinrichtung (4), wobei die Auswerteeinheit (2) einen Chip nach einem der Ansprüche 1 bis 7 umfaßt.

9. Funktionssteuereinrichtung (4) einer Nutzungsberechtigungskontrolleinrichtung zum Vergleichen einer intern erzeugten verschlüsselten Nachricht (H(Y)) mit einer erhaltenen verschlüsselten Nachricht (H(Y)) und zum Freigeben mindestens einer durch die Nutzungsberechtigungskontrolleinrichtung geschützten Funktion bei übereinstimmenden Nachrichten, wobei die Nutzungsberechtigungskontrolleinrichtung einen Chip nach einem der Ansprüche 1 bis 7 umfaßt.

10. Wegfahrsperre eines Kraftfahrzeugs, die benutzerseitig eine Schlüsseleinrichtung (5) und fahrzeugseitig eine Antenne, einer Auswerteeinheit (2) und einer Antriebsfreigabeeinrichtung (4) aufweist, wobei die Schlüsseleinrichtung (5) über eine Kommunikation über die Antenne durch die Auswerteeinheit (2) authentifizierbar ist und die Antriebsfreigabeeinrichtung (4) von der Auswerteeinheit (2) benachrichtigt wird, daß antriebsrelevante Funktionen freigegeben werden können, und wobei mindestens die Auswerteeinheit (2) einen Chip nach einem der Ansprüche 1 bis 7 umfaßt.

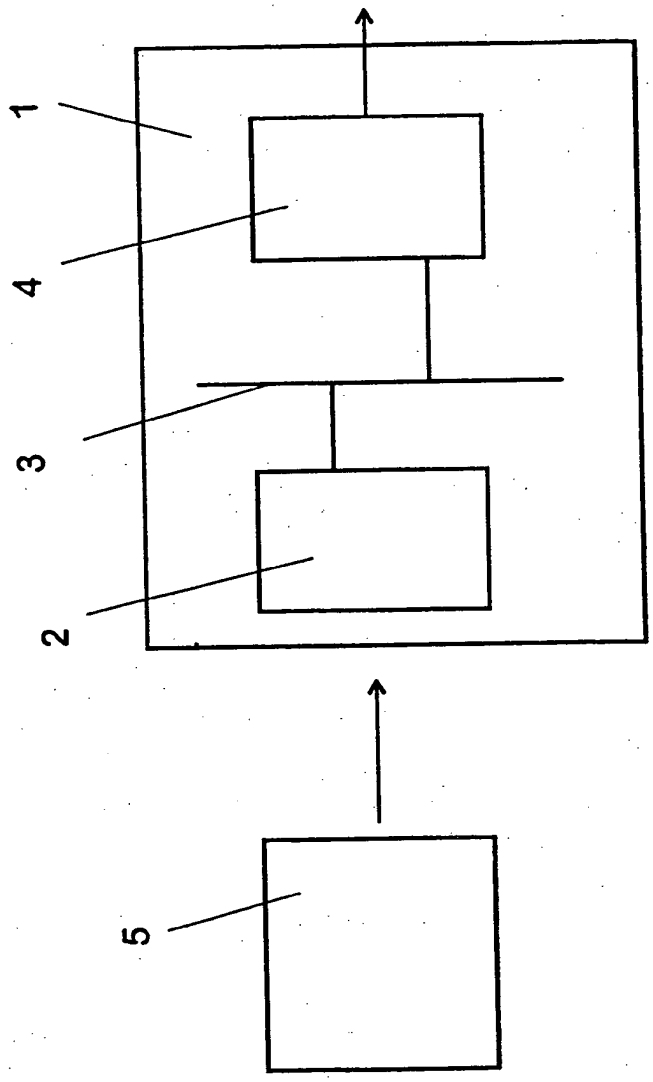

FIG. 1

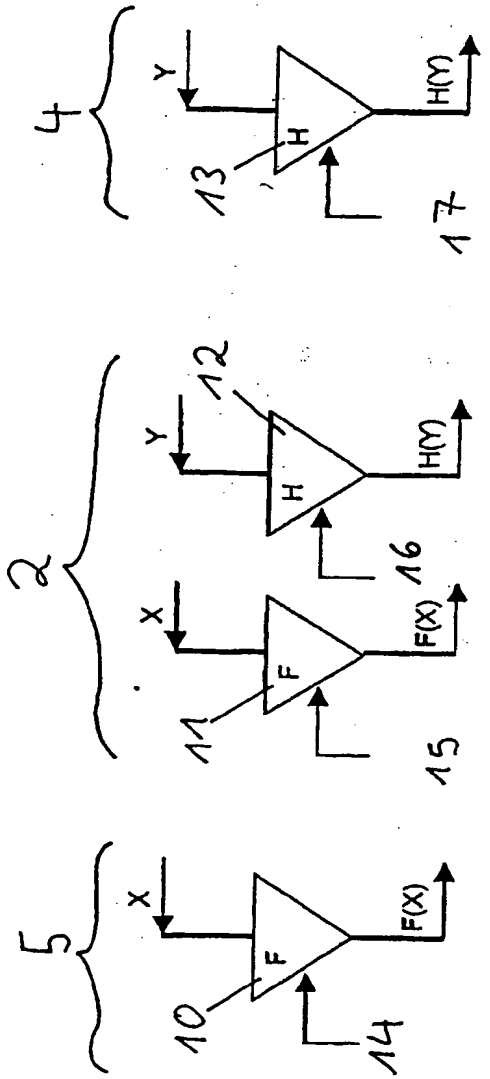

FIG. 2

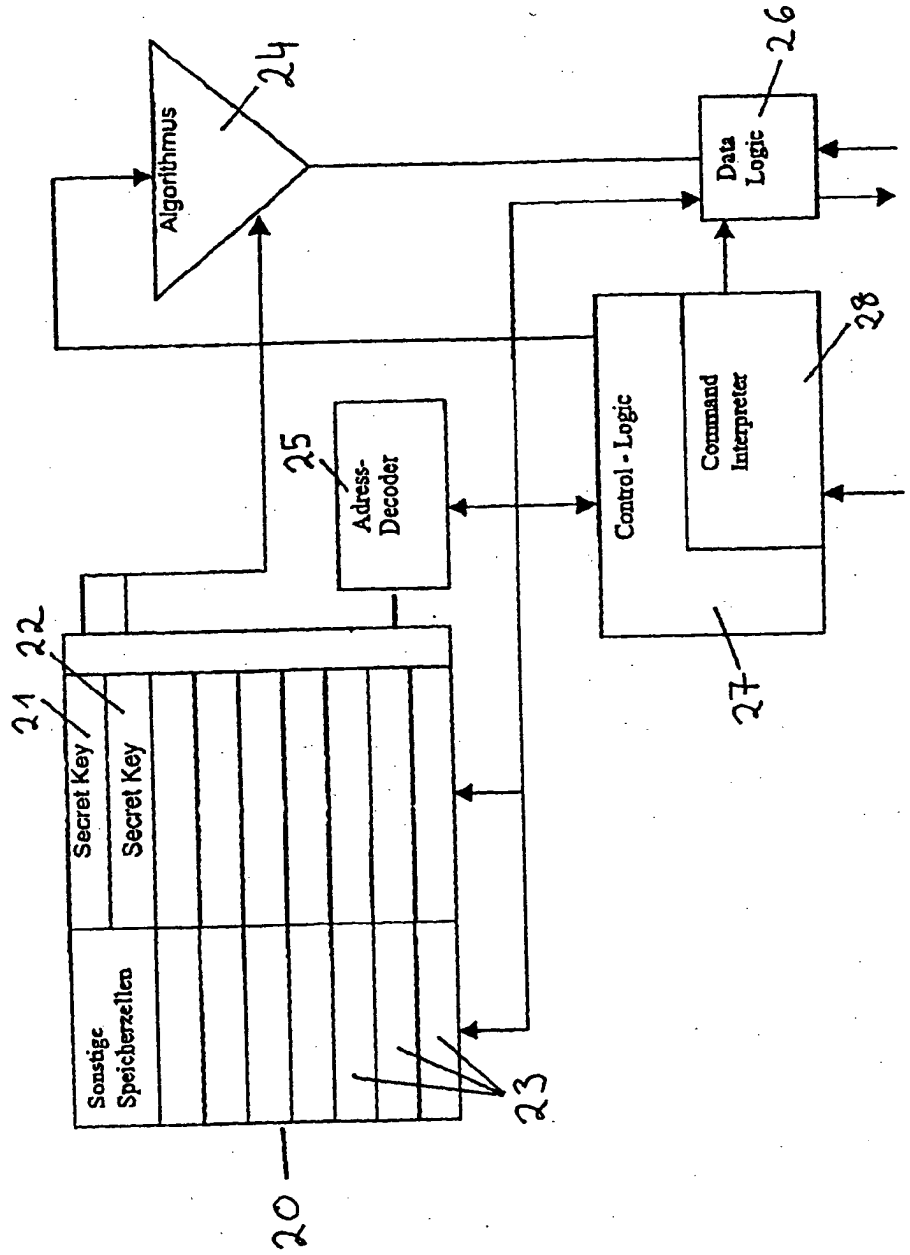
Algorithmus
24
Data Logic
26
Control - Logic
Command Interpreter
28
Adress-Decoder
25
27
21
22
Secret Key
Secret Key
Sonstige Speicherzellen
23
20

FIG. 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 098 472 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
03.07.2002 Patentblatt 2002/27

(51) Int Cl.[7]: **H04L 9/32**

(43) Veröffentlichungstag A2:
09.05.2001 Patentblatt 2001/19

(21) Anmeldenummer: **00123821.1**

(22) Anmeldetag: **02.11.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **03.11.1999 DE 19952841**

(71) Anmelder: **TeraTron GmbH**
51647 Gummersbach (DE)

(72) Erfinder:
- **Weiss, Bernd**
  51647 Gummersbach (DE)
- **Konrad, Reimund**
  51647 Gummersbach (DE)
- **Petsching, Wilfried**
  51702 Bergneustadt (DE)

(74) Vertreter: **Cohausz & Florack**
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(54) Chip für die Speicherung eines Secret Keys zur Verwendung in einer Nutzungsberechtigungskontrolleinrichtung

(57) Die Erfindung betrifft einen Chip für die Speicherung eines Secret Keys zur Verwendung durch einen Verschlüsselungsalgorithmus 24 zum Erzeugen einer verschlüsselten Nachricht in einer Nutzungsberechtigungskontrolleinrichtung. Um die durch eine Nutzungsberechtigungskontrolleinrichtung gewährte Sicherheit zu erhöhen, umfaßt der Chip erfindungsgemäß einen nichtflüchtigen Speicher 20, der mindestens einen Teilbereich 21, 22 aufweist, in dem ein Secret Key gespeichert ist, sowie einen mindestens einen Verschlüsselungsalgorithmus 24 realisierenden Hardwarebereich mit Zugriff zu dem Teilbereich 21, 22 des nichtflüchtigen Speichers 20 mit einem Secret Key.

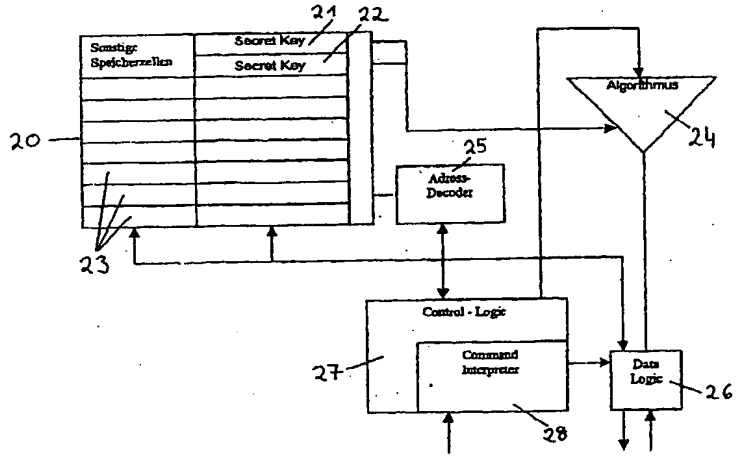

FIG. 3

EP 1 098 472 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 12 3821

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X Y	WO 98 34818 A (SIEDENTOP MICHAEL ;SCHREY ULRICH (DE); SIEMENS AG (DE)) 13. August 1998 (1998-08-13) * Zusammenfassung * * Seite 1, Zeile 10 - Seite 1, Zeile 30 * * Seite 3, Zeile 12 - Seite 4, Zeile 3 * * Seite 5, Zeile 24 - Seite 6, Zeile 11 * * Seite 6, Zeile 22 - Zeile 24 * * Seite 7, Zeile 18 - Zeile 25 * * Seite 8, Zeile 7 - Zeile 24 * * Seite 10, Zeile 4 - Seite 12, Zeile 7 * * Seite 13, Zeile 26 - Zeile 29 * * Seite 17, Zeile 24 - Seite 18, Zeile 6 * * Seite 20, Zeile 21 - Seite 21, Zeile 3 * * Seite 22, Zeile 19 - Seite 23, Zeile 16 * * Seite 24, Zeile 22 - Seite 25, Zeile 7 * * Abbildungen 1,2 *	1-3,5-7, 10 9	H04L9/32
X	US 5 742 236 A (CREMERS ROLF ET AL) 21. April 1998 (1998-04-21) * das ganze Dokument *	1,10	RECHERCHIERTE SACHGEBIETE (Int.Cl.7) H04L B60R G06F
X	EP 0 870 889 A (EATON CORP) 14. Oktober 1998 (1998-10-14) * Zusammenfassung * * Spalte 4, Zeile 20 - Spalte 9, Zeile 10 * * Spalte 9, Zeile 47 - Spalte 10, Zeile 25 * * Spalte 11, Zeile 23 - Zeile 46 *	1,3,5,7, 10	
Y A	DE 196 52 256 A (BOSCH GMBH ROBERT) 18. Juni 1998 (1998-06-18) * Zusammenfassung * * Spalte 1, Zeile 1 - Spalte 3, Zeile 61 * * Spalte 4, Zeile 28 - Zeile 53 *	9 8	

-/--

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	26. April 2002	Dujardin, C

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie,übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 12 3821

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
A	GB 2 296 804 A (JANSON NIGEL) 10. Juli 1996 (1996-07-10) * Seite 3, Zeile 6 - Zeile 26 * * Seite 6, Zeile 17 - Seite 7, Zeile 2 * * Seite 8, Zeile 23 - Seite 17, Zeile 15 *	8-10	
A	EP 0 835 790 A (DENSO CORP) 15. April 1998 (1998-04-15) * Zusammenfassung * * Spalte 1, Zeile 35-39 *	2,4	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.7)

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	26. April 2002	Dujardin, C

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.

EP 00 12 3821

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

26-04-2002

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9834818	A	13-08-1998	WO	9834818 A1	13-08-1998
			BR	9807669 A	15-02-2000
			EP	0958161 A1	24-11-1999
			JP	2001511090 T	07-08-2001
			US	6329909 B1	11-12-2001
US 5742236	A	21-04-1998	DE	4407966 A1	14-09-1995
			EP	0671528 A1	13-09-1995
			JP	8053962 A	27-02-1996
EP 0870889	A	14-10-1998	US	5937065 A	10-08-1999
			EP	0870889 A2	14-10-1998
DE 19652256	A	18-06-1998	DE	19652256 A1	18-06-1998
			AU	715336 B2	20-01-2000
			AU	5306598 A	15-07-1998
			WO	9826962 A1	25-06-1998
			EP	0942856 A1	22-09-1999
			JP	2001507649 T	12-06-2001
			SK	77599 A3	18-01-2000
GB 2296804	A	10-07-1996	KEINE		
EP 0835790	A	15-04-1998	EP	0835790 A2	15-04-1998
			JP	10175512 A	30-06-1998
			US	6160488 A	12-12-2000

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82